AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20) ___ Original __ Duplicate Original

# UNITED STATES DISTRICT COURT

for the

Central District of California



United States of America,

v.

HEREMOANA MII,

Defendant.

Case No. 2:24-mj-04806-DUTY

## CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about August 9, 2024, in the county of Los Angeles in the Central District of California, the defendant violated:

| *Code Section* | *Offense Description* |
|---|---|
| 21 U.S.C. § 841(a)(1) | Possession with Intent to Distribute Methamphetamine |

This criminal complaint is based on these facts:

*Please see attached affidavit.*

☒ Continued on the attached sheet.

/s/
*Complainant's signature*

Special Agent Michael DeNaro, HSI
*Printed name and title*

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: 8/11/2024

*Judge's Signature*

City and state: Los Angeles, California

Hon. Alka Sagar, U.S.M.J.
*Printed name and title*

AUSA: Kedar S. Bhatia (x4442)

# AFFIDAVIT

I, Michael DeNaro, being duly sworn, declare and state as follows:

## I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of a criminal complaint against Heremoana MII ("MII") for a violation of 21 U.S.C. § 841(a)(1) (Possession with Intent to Distribute Methamphetamine). This affidavit is also made in support of a search warrant for (i) a Black Apple iPhone 11 with IMEI 356863118770503 ("SUBJECT DEVICE-1"); and (ii) a White uleFone Note 17 Pro with IMEI 359505130070894 ("SUBJECT DEVICE-2" and, together with SUBJECT DEVICE-1, the "SUBJECT DEVICES") described in Attachment A, for the items to be seized described in Attachment B.

2. The property to be searched are the SUBJECT DEVICES, as described in Attachment A, which is incorporated herein by reference.

3. The items to be seized are the evidence, fruits, and instrumentalities of violations of Title 21, United States Code, Sections 841(a)(1) (possession with intent to distribute and distribution of controlled substances) and 846 (conspiracy to distribute controlled substances) (the "Subject Offenses"), as described in Attachment B, which is incorporated herein by reference.

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

## II. BACKGROUND OF AFFIANT

5. I am a Special Agent with Immigration and Customs Enforcement, Homeland Security Investigations ("HSI") and have been since September 2021. I am currently assigned to the HSI Office of the Assistant Special Agent in Charge Los Angeles International Airport ("LAX"), which is responsible for investigating federal crimes involving child exploitation, child pornography, cybercrimes, immigration crimes, human-rights violations, human smuggling, smuggling of narcotics, weapons, and other types of contraband, financial crimes, and various other violations of immigration and customs laws. Through my training, I have learned of HSI's criminal investigative authority, as well as investigative techniques. Prior to my appointment in the HSI LAX office, I was employed as a Police Officer with the West Newbury, Massachusetts, Police Department

from July 2017 to September 2021. I was also employed as a Police Officer with the Merrimack College Police Department in North Andover, Massachusetts, from September 2018 to December 2020.

6. As part of my duties as a Special Agent with HSI, I investigate various violations of federal law. During my tenure as a Special Agent, I have participated in various narcotics, financial, and child-exploitation investigations. As part of my law-enforcement experience, I have conducted physical surveillance, participated in the execution of search and arrest warrants, participated in the seizure of narcotics, and participated in various enforcement operations. My investigative experience detailed herein, as well as my training, experience, and conversations with other law-enforcement officers who are participating in this investigation, serve as the basis for the conclusions set forth herein.

## III. SUMMARY OF PROBABLE CAUSE

7. On August 9, 2024, MII attempted to travel from LAX to Tahiti International Airport via Air Tahiti on flight TN 101, which was scheduled to depart LAX at approximately 11:55 P.M.

8. During passenger risk analysis assessment, a Customs and Border Protection Officer ("CBPO") determined that MII was a high-risk passenger. This determination was made based on recent trends involving Tahitian methamphetamine smugglers. During a

border search of MII's checked luggage, another CBPO discovered two refillable bottles (one large and one small). The large refillable bottle was dark in color and was filled to the top with a crystalline substance. The small refillable bottle was silver in color and was filled with plastic. Inside the plastic was a crystalline substance. Based on my training and experience, I recognized the crystalline substance inside MII's luggage as methamphetamine.

9. After being detained, MII was advised of his Miranda rights and agreed to speak with law enforcement officers. Among other things, MII told me that the bag was his; he knew that the crystalline substance inside the bag was illegal narcotics; and he had attempted to conceal the methamphetamine inside the refillable bottles in the bag. MII also said that a particular individual provided him with money to buy the suspected methamphetamine, arranged MII's travel to the United States, and was going to pay MII approximately $60,000 upon his return to Tahiti with the narcotics.

10. CBP found two cellular devices among MII's belongings (defined below as the MII Cellphones). During his interview, MII gave HSI consent to search the cellular devices and voluntarily provided the passcode for the cellular devices. A preliminary search of one of the phones showed additional evidence of MII's

drug trafficking activities, including photographs of methamphetamine.

## IV. STATEMENT OF PROBABLE CAUSE

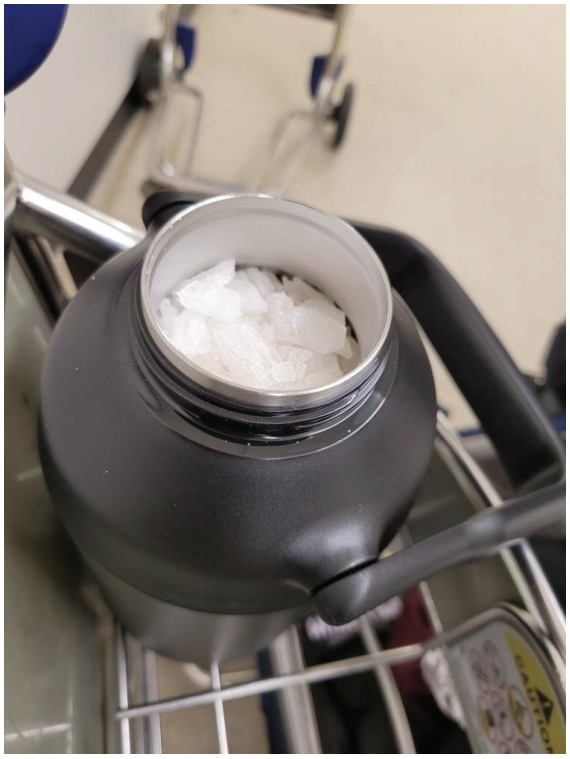
### A. MII Attempts to Smuggle Methamphetamine Through Screening Inside of His Checked Luggage

11. Based on my conversations with CBPO Supervisor Heather Sutton, CBPO Marionette Ventrice, and CBPO John Tionko, I know the following:

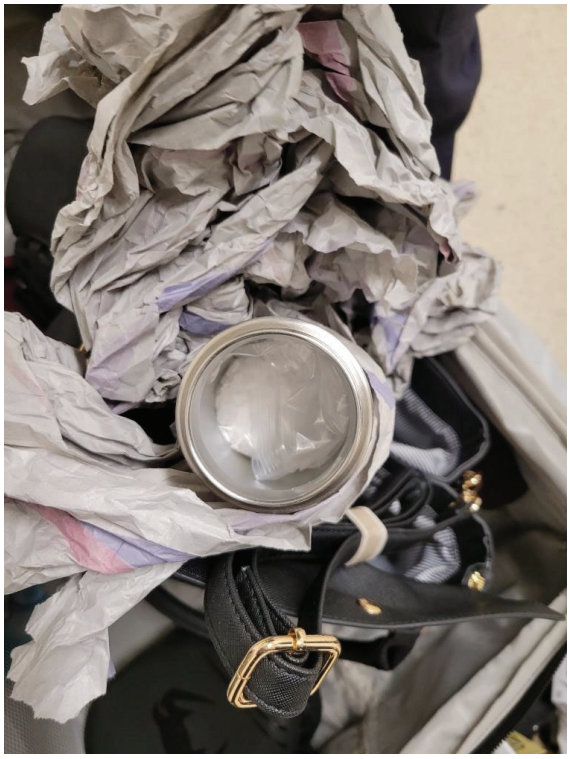
a. On August 9, 2024, MII attempted to travel from LAX to Tahiti International Airport via Air Tahiti Flight TN 101, which was scheduled to depart LAX at approximately 11:55 P.M. MII checked it at the Air Tahiti counter at LAX's Tom Bradley International Terminal ("TBIT"), and checked one piece of luggage for the flight (the "MII Luggage"). During a passenger risk analysis assessment, CBP determined that MII was a high-risk passenger and decided to conduct a search of MII's checked luggage pursuant to CBP's border search authority.

12. At approximately 10:00 P.M. on August 10, 2024, CBPO Ventrice performed an outbound search of the MII Luggage. When the MII Luggage was searched, CBPO Ventrice observed two refillable bottles inside the checked luggage, one large and one small (together, the "Refillable Bottles"). The large refillable bottle was dark in color and was filled to the top with a crystalline substance. The small refillable bottle was silver in

color and was filled with plastic, which contained a crystalline substance. The smaller refillable bottle was found inside of a black bag, stuffed with paper, inside of the MII Luggage. Images of the Refillable Bottles, with the crystalline substance are shown below:



*Larger Refillable Bottle*



*Smaller Refillable Bottle*

CBPO Ventrice also observed in MII's luggage men's clothing that appeared to be consistent with MII's size.

13. At approximately 11:00 p.m., on August 10, 2024, HSI Supervisory Special Agent Keith LaBranche, HSI Special Agents Adam Parada, Ian Albright, and I, and HSI LAX CBPOs responded to gate 204 in order to encounter MII. Upon MII's entrance to the jet bridge area, CBPOs encountered MII and searched his carry-on

luggage and his person. CBPOs found during this search, among other things, a passport showing MII's French citizenship as well as a boarding pass showing that MII was scheduled to depart on Air Tahiti Flight TN 101 at approximately 11:55 p.m. When officers searched MII's person and his carry-on luggage, they recovered two cellphones (the "MII Cellphones").

14. Based on my conversations with HSI SA Ian Albright, I know that SA Albright conducted a Thermo Scientific TruNarc test on the white crystalline substance that CBPO Ventrice discovered inside the refillable bottles that were themselves in the MII Luggage. The substance tested positive for the presence of methamphetamine.

15. CBPO Ventrice also weighed the methamphetamine inside the Refillable Bottles. The total approximate weight of the methamphetamine (including packaging) was approximately 1.57 kilograms. Based on my training and experience investigating narcotics offenses, this quantity of methamphetamine is consistent with an intent to distribute, not mere personal use.

**B. In an Interview, MII Admits to Knowingly Possessing the Methamphetamine for Distribution in Tahiti**

16. On August 10, 2024, HSI SA Adam Parada and I interviewed MII in U.S. Customs and Border Protection's main secondary inspection area at TBIT. MII was advised of his Miranda rights, agreed to speak with law enforcement officers,

and signed a Miranda waiver form.[1] The following is a summary of the interview and does set forth all the contents of the interview:

a. Initially during the interview, MII told SAs DeNaro and Parada a fictitious story about how he obtained the refillable bottles. He initially said, among other things, that a random man approached him and told him to take the bottles back home with him and to not look inside of them. Agents then left the room.

b. SA Parada and I later returned to speak with MII about his phones, the MII Cellphones. MII gave written and verbal consent for agents to search his cellphones, and he provided the passcodes for the cellphones. Agents again left the room.

c. MII later called SAs DeNaro and Parada back into the room where he was detained. He apologized to SAs DeNaro and Parada for "lying" and that he felt it was better to be honest. At this point in time, SA DeNaro re-read MII his Miranda rights

[1] MII indicated that he understood English, but asked that I speak slowly. Throughout the entire interview, MII was able to conversationally speak and understand English. I presented MII with a Miranda Rights Waiver form, which I read for MII in English. I then utilized the Google Translate application in order to translate the form into French for MII to read. In addition to hearing my oral statement of the Miranda form in English and signing the Miranda form in English, MII read the translation of the form in French and indicated that he understood his rights.

and he again agreed to waive those rights and speak to agents. MII said that he was currently employed as an emergency medical technician at the Tahiti International Airport; that he had traveled to Los Angeles by himself; and that the trip was paid for and arranged by an individual who used a particular moniker ("CC-1"). CC-1 arranged for him to meet another individual ("CC-2") to buy the narcotics. MII did, in fact, meet with CC-2 and received the narcotics. MII saw the drugs and knew what he was purchasing was drugs, and he put the drugs into the Refillable Bottles himself.

d. MII also admitted that the bag in which CBPO Ventrice discovered the methamphetamine, i.e., the MII Luggage, was his bag and that he knew that it was illegal to transport the drugs. MII also said that agents would find some pictures of the drugs on the phone that he took.

17. As set forth above, MII gave HSI LAX verbal and written consent to review the MII Cellphones. MII also voluntarily provided me with the passcodes to both cellular devices. I manually searched SUBJECT DEVICE-1 and observed multiple pictures of suspected methamphetamine in his photo gallery.

## V. TRAINING AND EXPERIENCE ON DRUG OFFENSES

18. Based on my training and experience and familiarity with investigations into drug trafficking conducted by other law enforcement agents, I know the following:

a. Drug trafficking is a business that involves numerous co-conspirators, from lower-level dealers to higher-level suppliers, as well as associates to process, package, and deliver the drugs and launder the drug proceeds. Drug traffickers often travel by car, bus, train, or airplane, both domestically and to foreign countries, in connection with their illegal activities in order to meet with co-conspirators, conduct drug transactions, and transport drugs or drug proceeds.

b. Drug traffickers often maintain books, receipts, notes, ledgers, bank records, and other records relating to the manufacture, transportation, ordering, sale and distribution of illegal drugs. The aforementioned records are often maintained where the drug trafficker has ready access to them, such as on their cell phones and other digital devices.

c. Communications between people buying and selling drugs take place by telephone calls and messages, such as e-mail, text messages, and social media messaging applications, sent to and from cell phones and other digital devices. This includes sending photos or videos of the drugs between the seller and the buyer, the negotiation of price, and discussion

of whether or not participants will bring weapons to a deal. In addition, it is common for people engaged in drug trafficking to have photos and videos on their cell phones of drugs they or others working with them possess, as they frequently send these photos to each other and others to boast about the drugs or facilitate drug sales.

d. Drug traffickers often keep the names, addresses, and telephone numbers of their drug trafficking associates on their digital devices. Drug traffickers often keep records of meetings with associates, customers, and suppliers on their digital devices, including in the form of calendar entries and location data.

e. Individuals engaged in the illegal purchase or sale of drugs and other contraband often use multiple digital devices.

## VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

19. As used herein, the term "digital device" includes the SUBJECT DEVICES, which are cellphones.

20. Based on my experience, training, and familiarity with cellphones, I am aware of the following:

a. Cellphones frequently have telephone directory features, as well as methods to learn the call number associated with each cellphone, such as caller-identification features. Cellphones also typically contain records of recent call

activity, both incoming and outgoing calls, and lists of stored telephone numbers and other identifying information, such as names. Cellphone users often maintain lists, such as address books or contact information, that are stored on the cellphone or its SIM or memory card.

b. Cellphones typically have voicemail or voice-mailbox features that allow callers to leave voice and/or alphanumeric messages if the cellphone user does not answer. Voicemail is typically stored on the computer network of the provider of the cellphone's telephone service, which network is external to the cellphone, but may also be stored on the cellphone itself.

c. Cellphones typically have messaging capabilities, including text, data, chat, digital photographs and video, MMS (i.e., multimedia messaging service), and SMS (i.e., short message service) messaging and email (collectively, "text messages"), that permit the cellphones user to send and receive text messages, including messages with digital photographs and video attached. Text messages and any attachments are typically stored on the computer network of the provider of the cellphone's telephone service, which network is external to the cellphones, but may also be stored on the cellphones itself.

d. Cellphones often have electronic calendar features that allow the cellphone user to schedule appointments

and meetings. Cellphones users often use that feature to remind themselves of meetings and appointments with friends and confederates.

e. In addition to voicemail and text-messaging features, cellphones typically offer capabilities such as sending and receiving email, and accessing and downloading information from the Internet.

f. Cellphones may have applications installed, including social media and messaging applications that permit the user to communicate with contacts using these applications.

g. Cellphones with camera functions permit the cellphone user to take photographs and videos, which are stored on the cellphone itself.

h. Cellphones may record location data that records where the user has carried or used the cellphone.

i. The information described above usually remains accessible in the cellphone's memory even if the cellphone has lost all battery power and has not been used for an extended period of time.

21. Based on my training and experience, I also know that, where electronic devices such as the Subject Device are used in furtherance of criminal activity, evidence of the criminal activity can often be found months or years after the criminal activity occurred. This is typically true because:

a. Electronic files can be stored on an electronic device for years at little or no cost and users thus have little incentive to delete data that may be useful to consult in the future.

b. Even when a user does choose to delete data, the data can often be recovered months or years later with the appropriate forensic tools. When a file is "deleted" on an electronic device, the data contained in the file does not actually disappear, but instead may remain on the device, in "slack space," until it is overwritten by new data that cannot be stored elsewhere on the device. Similarly, files that have been viewed on the Internet are generally downloaded into a temporary Internet directory or "cache," which is only overwritten as the "cache" fills up and is replaced with more recently viewed Internet pages. Thus, the ability to retrieve data from an electronic device depends less on when the file was created or viewed than on a particular user's operating system, storage capacity, and computer habits.

c. In the event that a user changes electronic devices, like a cellphone, the user will typically transfer files from the old device to the new device, so as not to lose data.

22. Based on the foregoing, I respectfully submit that there is probable cause to believe MII is engaged in the Subject

Offenses, and that evidence, fruits, and/or instrumentalities of the Subject Offenses will be found on the SUBJECT DEVICES. In addition, based on the foregoing, I respectfully submit there is probable cause to believe that the SUBJECT DEVICES constitute instrumentalities of the Subject Offenses and are therefore subject to seizure.

23. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been

used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

24. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it can take a substantial period of time to search a digital device for many reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

## VII. CONCLUSION

25. For all of the reasons described above, I submit that there is probable cause to believe that MII has committed a violation of 21 U.S.C. § 841(a)(1) (Possession with Intent to Distribute a Controlled Substance).

26. Further, there is probable cause to believe that the items listed in Attachment B, which constitute evidence, fruits,

and instrumentalities of violations of the Subject Offenses will be found on the SUBJECT DEVICES, as described in Attachment A.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 11th day of August, 2024.

HON. ALKA SAGAR
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

PROPERTY TO BE SEARCHED

The following digital devices (together, the "SUBJECT DEVICES"), which were seized on August 9, 2024, and are currently maintained in the custody of Homeland Security Investigations in Los Angeles, California:

1. A Black Apple iPhone 11 with IMEI 356863118770503; and
2. A White uleFone Note 17 Pro with IMEI 359505130070894.

**ATTACHMENT B**

**A. ITEMS TO BE SEIZED**

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of Title 21, United States Code, Sections 841(a)(1) (possession with intent to distribute and distribution of controlled substances) and 846 (conspiracy to distribute controlled substances) (the "Subject Offenses"), from June 1, 2024, to August 9, 2024, namely:

a. Records reflecting the possession, purchase, transfer, or sale of narcotics, or attempts to do the same.

b. Records reflecting proceeds from the Subject Offenses.

c. Records related to communications with co-conspirators in the Subject Offenses.

d. Records related to the identities and roles of conspirators or aiders and abettors to the Subject Offenses.

e. Records related to the nature and development of the relationships among co-conspirators in and witnesses to the Subject Offenses, such as personal, social, and familial connections, prior dealings, financial compensation, and loans.

f. Records reflecting efforts to conceal the Subject Offenses or avoid detection by law enforcement, such as efforts to conceal narcotics for transportation on commercial aircraft.

g. Records related to motive for the Subject Offenses, including but not limited to communications relating to debts or other financial obligations.

h. Evidence of efforts to use and use of encrypted applications, programs, and devices.

i. Records related to the location of other evidence of the Subject Offenses, including but not limited to communications reflecting registration of online accounts potentially containing relevant evidence and financial accounts.

j. Records related to who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence.

k. Records related to the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.

l. Records related to attachment of other devices.

m. Records related to counter-forensic programs (and associated data) that are designed to eliminate data from the device.

n. Records related to the times the device was used.

o. Records related to passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device.

p. Records related to applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it.

q. Records related Internet Protocol addresses used by the device.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, messages, emails, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. Any SUBJECT DEVICE which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.

4. With respect to any SUBJECT DEVICE containing evidence falling within the scope of the foregoing categories of items to be seized:

a. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted;

b. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the attachment of other devices;

d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

e. evidence of the times the device was used;

f. applications, programs, software, documentation, manuals, passwords, keys, and other access devices that may be necessary to access the device or data stored on the device, to run software contained on the device, or to conduct a forensic examination of the device;

g. records of or information about Internet Protocol addresses used by the device.

5. As used herein, the terms "records," "information," "documents," "programs," "applications," and "materials" include records, information, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

**B. SEARCH PROCEDURE FOR THE SUBJECT DEVICES**

6. In searching the SUBJECT DEVICES (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") may search the SUBJECT DEVICES capable of being used to facilitate the above-listed violations or containing data falling within the scope of the items to be seized.

b. The search team will, in its discretion, either search the SUBJECT DEVICES where they are currently located or transport them to an appropriate law enforcement laboratory or similar facility to be searched at that location.

c. The search team shall complete the search of each SUBJECT DEVICE as soon as is practicable but not to exceed 120 days from the date of issuance of the warrant. The government will not search the digital device and/or forensic images thereof beyond this 120-day period without obtaining an extension of time order from the Court.

d. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each SUBJECT DEVICE capable of containing any of

the items to be seized to the search protocols to determine whether the SUBJECT DEVICE and any data thereon falls within the scope of the items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of the items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase," "Griffeye," and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

e. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

f. If the search determines that a SUBJECT DEVICE does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the SUBJECT DEVICE and delete or destroy all forensic copies thereof.

g. If the search determines that a SUBJECT DEVICE does contain data falling within the list of items to be seized,

the government may make and retain copies of such data, and may access such data at any time.

h. If the search determines that a SUBJECT DEVICE is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

i. The government may also retain a SUBJECT DEVICE if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

j. After the completion of the search of a SUBJECT DEVICE, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

7. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the

government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

8. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.